Achieving 21 CFR Part 11 Compliance with Appian

Software performance in the life sciences industry has extremely high standards. The FDA and other regulatory bodies require software used in core areas of the business (e.g., clinical, manufacturing, product safety, etc.) comply with specific guidelines (e.g., GxP and 21 CFR Part 11), be validated to perform as intended, and be re-validated whenever changes are made. Ensuring software applications meet these criteria can be a challenge, especially for commercial off-the-shelf applications, which are intended to address defined, specific challenges.

In contrast, Appian's modern application platform is designed to be open, easily validated, easily updated, and re-verified as needed, leveraging out-of-the-box traceability, security, and accountability capabilities. This platform includes a complete audit trail of user access, data collected, and changes made, including time-stamps. Appian uses PCI DSS-compliant login and password management to tightly control user access. Built-in security measures ensure only authorized individuals can use the system, electronically sign a record, access the process, alter a record, or perform the operation at hand. Reports can be generated on any aspect of the system with output suitable for inspection, review, and copying by regulatory agencies.

This paper explores the details of the Appian features for compliance and validation and explains why Appian is a low risk choice for software applications in core areas of the commercial life sciences industries.

INTRODUCTION AND BACKGROUND

The Food and Drug Administration (FDA) introduced 21 CFR Part 11—originally proposed to promote the expanded use of technology in the pharmaceutical industry—as a requirement for commercial life science companies that maintain FDA-required records and signatures in electronic format to meet specific standards and comply with good clinical, laboratory, and manufacturing practices. The regulation is considered critically important by the FDA, as life science applications affecting a production environment can have catastrophic consequences if not regulated, up to and including increased probability of death or disability.

The primary goals of this regulation are to ensure:

- Data integrity
- Changes made to the system are documented, reasoned, and non-repudiated
- Computer systems used are trustworthy
- Applications are validated to intended use

The stringent quality requirements in FDA-regulated industries require life science companies to deploy software with specific controls and procedures that satisfy these requirements. Evidence of compliance with these controls and procedures must be documented and must pass regulatory audits by trained inspectors. Failure to do so results in significant FDA sanctions and/or financial penalties.

21 CFR Part 11 applies to any paper records required by statute or agency regulations. It supersedes any existing paper record requirements, articulating that electronic records may be used in lieu of paper records. The FDA guidance documents for 21 CFR Part 11 provide specific criteria under which the FDA will consider electronic records to be equivalent to the same paper records, and electronic signatures equivalent to traditional and written signatures. It also introduces strict administrative controls designed to make electronic signatures as secure and legally binding as handwritten signatures, and resulting in electronic records being considered a suitable replacement for paper. Electronic signatures that meet the requirements of the rule are considered to be equivalent to full handwritten signatures, initials, and other general signings required by agency regulations.

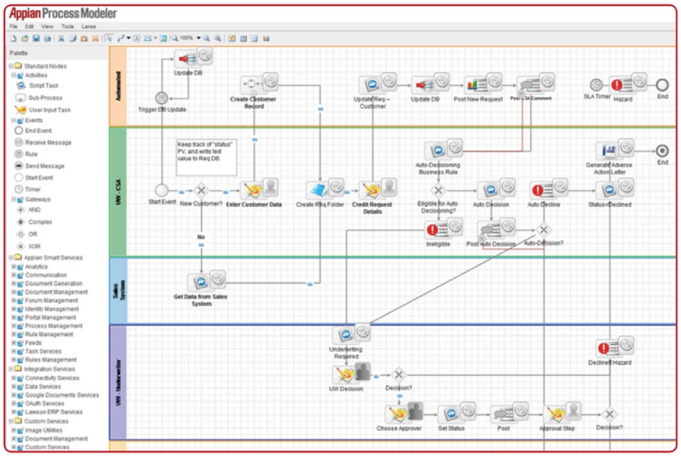
Independent of whether a company uses electronic signatures, 21 CFR Part 11 is still enforced when computer systems are used to create records in electronic form associated with the GxP environment. Computer systems used in this category must have the following controls:

1. Ability to generate accurate and complete copies of records
2. Availability of time-stamped audit trails
3. Protection of records to enable accurate and ready retrieval
4. Enforced system access and authoring checks

HOW APPIAN SUPPORTS 21 CFR PART 11 COMPLIANCE

Because of the language in the 21 CFR Part 11 guidance documents, there are likely to be significant variations in the way this rule will be interpreted across the commercial life sciences industry. Appian provides all of the capabilities required by the FDA to fully achieve 21 CFR Part 11 compliance (regardless of the interpretation of the requirements). It has been proven to stand up to close scrutiny by trained inspectors.

Appian achieves this level of regulatory oversight by providing full audit trail capabilities down to the data field layer, ensuring complete transparency of who has entered data or changed data/rules and when. Appian also allows its customers to proactively address the evolving nature of regulatory compliance. The software is entirely configurable, allowing organizations to have and change their own unique solutions without tremendous effort (unlike custom coding or commercial-off-the-shelf (COTS) solutions).



Keep track of "status" PV, and write text value to Req DB.

Appian's visual modeling environment takes the place of computer code, allowing business users and inspectors to easily understand how a specific app works

Any app created in Appian has these features built in. Appian can be applied to almost any process need in life sciences. Creating multiple apps in Appian provides life science companies with great information technology leverage, while extending compliance features created in one application for use in others.

This innovative approach leveraging state-of-the-art technology to more efficiently manage multiple business problems ultimately improves the FDA inspection process: There is one validated system of record, and all of the corresponding documentation is maintained electronically in one place throughout the retention period. Over the long term, this approach promotes significant savings and reduced expenditure of effort for everyone involved, including the FDA.

DEPLOYING APPIAN TO ENSURE TECHNICAL COMPLIANCE WITH 21 CFR PART 11

The remainder of this document describes how Appian can be deployed to demonstrate technical compliance with U.S. FDA CFR Part 11 Electronic Records, Electronic Signatures Final Rule, and several international good x practice (GxP) guidelines with similar requirements. Background information about the regulation, as well as examples of electronic records and signatures within Appian are included.

THE RELATIONSHIP BETWEEN CORPORATE POLICIES AND PROCEDURES FOR 21 CFR PART 11 COMPLIANCE AND THE SOFTWARE DEVELOPMENT LIFE CYCLE

Education/Training/Policies

The success of any electronic solution involving CFR Part 11 compliance will be measured by more than just the performance of the selected solution. It also will be measured by how effectively the life science organization's internal personnel use the solution.

Appian education services for life sciences organizations focus on using Appian technology to successfully deploy CFR Part 11 compliant solutions. This is accomplished through a comprehensive curriculum of courses and learning paths that teach both business and information technology (IT) users how to effectively use, configure, and develop Appian software.

Before any electronic solution is deployed, a company's leadership must identify the best approach to ensure users understand how to use the system, as well as the specific internal policies that must be followed to avoid unrestricted access. These activities are the responsibility of the organization creating processes using Appian software and are not directly related to software system capabilities. However, Appian does provide its clients best practices for standard operating procedures (SOPs) and training activities to achieve compliance. The table below describes various activities commercial life science companies should conduct when deploying an electronic solution that will comply with 21 CFR Part 11 and how Appian assists.

ACTIVITY	HOW APPIAN CAN ASSIST
Determine persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. Appian works with customers to ensure all users, process designers, developers, and administrators have appropriate knowledge to easily build and deploy secure, process-based electronic applications.	Appian works with customers to ensure all users, process designers, developers, and administrators have appropriate knowledge to easily build and deploy secure, process-based electronic applications.
Establishment of (and adherence to) written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures to deter record and signature falsification.	A process designer using Appian can enable any number of steps, inputs, checks, and rules to ensure adherence to the organization's written policies. Security elements of Appian ensure only registered users can use their specific electronic signature.
Limiting system access to authorized individuals.	Appian has built-in authorization capabilities to handle complex group and role structures to model any secure processes. Appian can be integrated with corporate directory servers for enterprise authentication.
Use of authority checks to ensure only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Appian handles this two fold, first through directory integration and secondly through native support for PCI DSS Compliance for authentication. When integrated with a directory server such as LDAP, the security controls for password aging can be set according to rules in the directory or single-sign-on application. For instances where Appian is leveraged as the authentication module (e.g., in the cloud offering) Appian enables compliance with requirement 8 of PCI Data Security Standard (PCI DSS) v1.2.1 which addresses user access and password management.
Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and immediately and urgently detect and report any attempts at unauthorized use to the system security unit, and, as appropriate, to organizational management.	Appian has native support for PCI Data Security Standards Compliance for authentication. These last three items typically are managed by the organization using the password and loss prevention controls in place.
Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification.	Appian has native support for PCI Data Security Standards Compliance for authentication. These last three items typically are managed by the organization using the password and loss prevention controls in place.

VALIDATING 21 CFR PART 11 COMPLIANT SOLUTIONS TO ENSURE THE SYSTEM WORKS AS INTENDED

As mentioned previously, and individual company approach 21 CFR Part 11 compliance is based on the company's interpretation of the FDA Guidance Documents, as well as internal efforts to adopt industry best practices. One important component less likely to have interpretation variability is Validation. An important element for any electronic solution is documenting how the electronic application fulfills its intended purpose.

Validation

Appian vigorous tests its BPM suite to ensure the underlying platform works as intended and is continuously in compliance. Specific process applications built on the Appian platform must be independently validated so they work as intended. The individuals who create an Appian-based application, whether at the end-user organization, Appian, or a third-party organization must create a testing plan to validate the application works as intended.

Appian has a number of built-in features that streamline the work involved in Validation. Appian Professional Services can assist in development of such plans, and the Appian Labs Program is available to help clients be confident in their approaches.

Appian releases updated versions of its software on a regular, quarterly basis. These updates are to the underlying platform; All have backwards compatibility so applications built on older versions of Appian will run on newer versions. Since an upgrade of the Appian platform does not make any changes to an application, it should have no impact on validation. Clients that want to be extra conservative can simply re-run the original validation process used for an application.

HOW APPIAN'S PLATFORM AND SERVICES TEAM HELPS CLIENTS VALIDATE THEIR APPLICATIONS

The best way to ensure a software application is validated for use in life sciences is to begin the actual development with that goal in mind. Just as software developers design ways to test code being written works as intended, application creators must design applications so others can easily validate performance is as intended.

For most commercial off-the-shelf applications, this is a challenge as their inner workings are proprietary and not open for inspection. For these applications, all that can be observed is the end result of the software's functions. Conversely, with Appian, complete functionality of any application built on the platform is open and exposable through automatically generated documentation. This documentation, as well as the ability to monitor specific process instances in a graphical environment, make validation much easier than with traditional software applications.

Appian's software is designed to allow most business analysts and IT staff to work side-by-side to develop specific applications. The Appian modeling environment serves as a process monitor. When combined with automatically generated documentation, this enables easy validation and re-validation. While application creation can be done without involvement from Appian's professional services team, it is recommended to keep Appian staff involved to benefit from the team's combined hundreds of years experience. Doing so keeps applications designed in the easiest way to support on-going validation and following best practices gleaned from the many other engagements in the life sciences industry.

System Security, Integrity, and Access

The Appian security model operates on the principle that a user without the proper rights assignment must be prevented from accessing a particular document or object. Objects attached to processes or nodes always maintain individual security parameters separate from the process to which they are attached. For instance, if a user is assigned a task that includes an attached document the user does not have rights to view, the document is not displayed.

Appian implements its security via Access Control Lists (ACLs) for each of its components. The concept of user permissions is strongly linked to groups, managed in Appian's internal Identity Management System.

Change Controls (Master Record and Documents)

Any desired change controls can be instrumented and enforced through the use of Appian processes. The use of structured processes prevents untraceable ad hoc actions from being taken in the system.

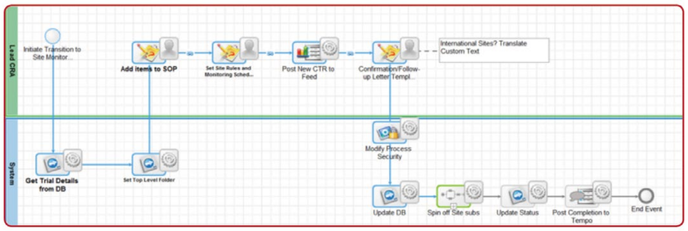
All Appian processes are secured and targeted to the right personnel at the right time, ensuring proper hand-offs and sequencing of activities occur. All process actions—whether human or system activities—are fully audited and logged automatically. Appian provides a comprehensive audit trail that captures:

- Activity date and time
- Object or entity against which action was taken
- Name of the action
- Actor (human or system) that took the action
- Resulting properties of the action

All of this data may be viewed by authorized system administrators through the process details dashboard. This dashboard provides not only a view into the audit trail, but also a list of currently active tasks, the current state or value of every process variable, as well as any attachments (records, documents, images, etc.) or notes associated with the process. All process details and the audit trail are retained online as long as desired and may be configured on a process-by-process basis. Archiving removes process information from the live view, but that information is retained on disk. Archived processes may be retrieved in the future for review. Additionally, any process data may be written to a third-party data store or database for reporting or other access purposes.

OPERATIONAL SYSTEM CHECKS TO ENFORCE PERMITTED SEQUENCING OF STEPS AND EVENTS

Appian provides a comprehensive process modeling and execution environment that enables process authors to design and deploy structured and secure processes. Any system checks or sequencing of events needed or desired may be incorporated to meet the operational needs of a 21 CFR Part 11 system. As an open-ended platform designed to be flexible and configurable to individual customer needs, Appian can be configured to provide varying degrees of rigidity or enforcement of policy secured to the individual user or group.


Lead CRA
System
Initiate Transition to Site Monitor...
Add items to SOP
Set Site Rules and Monitoring Sched...
Post New CTR to Feed
Confirmation/Follow-up Letter Templ...
International Sites? Translate Custom Text
Get Trial Details from DB
Set Top Level Folder
Modify Process Security
Update DB
Spin off Site subs
Update Status
Post Completion to Tempo
End Event

FEATURES OF APPIAN'S SOFTWARE FOR 21 CFR PART 11 COMPLIANCE

Password Security

Controls for identification codes/passwords
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

Password uniqueness can be managed within Appian, although this functionality is typically deferred to the directory server (i.e., the keeper of all passwords in the organization).

Ensuring that identification code and password issuances are periodically checked, recalled, or revised, (e.g., to cover such events as password aging).

Appian handles this in two ways: first, through directory integration, and secondly through native support for PCI DSS Compliance for authentication. When integrated with a directory server such as LDAP, security controls for password aging may be set according to rules in the directory or single-sign-on application. For instances where Appian is leveraged as the authentication module—such as in the cloud offering—Appian enables compliance with requirement 8 of PCI Data Security Standard (PCI DSS) v1.2.1, which addresses user access and password management.

- Password Management: Complexity requirements for user passwords can be configured:
  - Minimum number of characters
  - Minimum number of numeric characters
  - Minimum number of alphabetic characters
  - Minimum number of special characters required
  - Number of past passwords to check for uniqueness
  - Maximum password age (or password expiration)

- Reset Password Functionality
  - System administrators can reset user passwords
  - A temporary password is automatically assigned and sent to the user in an email

- Locking User Accounts on Failed Access Attempts
- Deactivating Inactive User Accounts

User and Group Logging:

How does Appian log when a group or user is removed?

The best practice for managing users and tracking when users or groups are created or deactivated in Appian is to leverage Appian process models for managing users. This enables a significant level of control over user activation and deactivation. A series of process applications has been developed for this very purpose and have been deployed in a number of instances. This approach enables detailed tracking, specific to each application.

Restricted Access:

Security to ensure only authorized individuals can use the system, electronically sign a record, access the process, alter a record, or perform the operation at hand.

Appian has built-in authorization capabilities to handle complex group and role structures to model secure processes. Appian additionally may be integrated with corporate directory servers for enterprise authentication.

Audit Trails:

Security to ensure only authorized individuals can use the system, electronically sign a record, access the process, alter a record, or perform the operation at hand.

Appian has complete audit trails of all process data and variables, including timestamps indicating when each data has changed in value, the individual who made the change, and the change in data itself.

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.
With the proper authorization levels, all data may be easily exported from and monitored within Appian.

Protection of records to enable their accurate and ready retrieval throughout the records retention period.
All data in Appian may be secured down to the row level. Additionally, data may be persisted in independent third party database systems with additional and separate security and retention controls.

Use of appropriate controls over systems documentation.
Appian provides full audit trails for both the in-flight process data, as well as the process and rule definitions. Changes application artifacts, including processes, rules, data, and documents, are recorded and auditable inside Appian process audit trails and system log files.

Electronic Signatures Capabilities:

Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- The printed name of the signer
- The date and time when the signature was executed
- The meaning (such as review, approval, responsibility, or authorship) associated with the signature specific to each application.

Appian allows process designers to easily build and deploy processes that collect the name of the signer, when the signature was performed, and the meaning of the signature (approving, reviewing etc.). This information is tracked in the Appian process engine for later retrieval.

The items identified above are subject to the same controls as electronic records and are included as part of any human readable form of the electronic record (such as electronic display or printout).

Signature/Record Linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied or otherwise transferred so as to falsify an electronic record by ordinary means.

The record of the signature is kept in the secure Appian process engine. Each deployment of Appian must be set up following the instructions of our administration guide to ensure all ports and access to the backend system are secure.

Electronic Signatures

Appian is fully capable of fulfilling electronic signature requirements that meet 21 CFR Part 11 requirements. Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. Appian's experience to date suggests interpretation of Part 11 as it relates to electronic signatures varies considerably from company to company. In that regard, Appian has implemented various electronic signatures, ranging from checking a box to multifactorial authentication pursuant to 21 CFR Part 11 requirements.

Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

Uniqueness of the signature is typically handled by the directory server (i.e. Active Directory, LDAP, etc.). Appian can create a separate account for each user to ensure all signatures are unique.

Electronic Signature Components and Controls

Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(2) When an individual executes a series of signings during a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(3) When an individual executes one or more signings not performed during a single continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

By default, Appian only requires authentication at the beginning of a series of signings (i.e. when an individual logs into the system). However, to support this functionality, Appian has user input components to ensure that individuals authenticate on every submit (or a subset of submits) to the process engine. This approach to electronic signature greatly reduces the probability of a session hijacking.

Signature/record linking: Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

While the onus is largely on the company to achieve this, Appian gives its customers the ability to do both. This is done several ways. First, Appian software has the ability to validate/audit data at any point and can generate read-only records/documentation to capture electronic signatures at specific milestones. If digital signatures are required, the use of third-party applications may be integrated to represent the PKI. This helps customers trace any piece of data that may have changed throughout the process and, more importantly, identify who did what, when.

When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

Appian's base security features include the ability to configure time-outs for system inactivity over any length of time, as well as the requirement of specific procedures for log-in and log-out. Appian allows for custom configuration of automatic time- or log-outs to ensure no user credentials are compromised. Processes also may be designed to require additional credentials at various steps or stages for user authentication. If a third-party electronic signature solution is being used, Appian also has the flexibility to add signature challenges in various forms, designing a process that defines when and how an electronic signature needs to occur. All information is captured in the Appian log and available in an audit trail.

Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

The flexibility of the Appian platform allows customer designers to include process behaviors that would prevent the need to have this level of collaboration. (For example, Appian provides process escalation and exception management capabilities that allow administrators to reassign or delegate tasks if someone is out of the office.) More importantly, all exceptions are traced in the audit log. In addition, reassignments can be messaged through emails or alerts to increase transparency.

Appian Also Simplifies the Regulatory Audit Process

In the event of a regulatory audit, Appian provides comprehensive audit trail, security, analytics, and records capabilities out-of-the-box. Appian uses industry-standard log-on capabilities that can be shared. This enables customers to provide comprehensive records and reports to auditors proactively. Some key features of Appian enable customers to build reports and dashboards to illustrate compliance. If compliance is ever compromised, Appian can be configured to generate reports that track how alerts and flags are resolved. The intelligence capabilities of Appian enable users to build customized processes ahead of time to avoid problems in the future. Appian gives its users the ability to more easily meet regulatory requirements, based on individual needs.

CONCLUSION

Compliance to 21 CFR Part 11 requires a set of activities and controls that FDA-regulated companies must follow for any electronic record or signature connected to the GxP environment. The objective of these activities is to document evidence that an application generating FDA regulated data fulfills its intended purpose; the data itself is valid; and the data has integrity. The primary intent of this regulation is to avoid problems that could have a major impact on patient safety and public health. Using state-of-the-art software like Appian is an important step to consistently achieve compliance.

It is important to note 21 CFR Part 11 compliance is about more than just testing and controls. Compliance with this requirement involves a variety of equally important elements that need to be conducted both pre and post-application deployment. Appian has positioned itself as a leader in the commercial life sciences industry by not only deploying compliant solutions but also partnering with relevant industry organizations on this very important topic. Appian's software meets every aspect of 21 CFR Part 11 compliance, as demonstrated above.

Appian has helped many organizations implement systems that follow stringent quality guidelines. Because Appian is a platform for building modern process applications, it provides a much greater level of transparency into the inner workings of the software than any pre-built, commercial-off-the-shelf application, which often needs subsequent, complex customizations to be able to address more specific organizational challenges. Appian converges process, collaboration, compliance, and data on a single, integrated software platform to help our life sciences customers create 21 CFR Part 11 compliant applications.

NOTES

NOTES

Appian

Appian provides a leading low-code software development platform that enables organizations to rapidly develop powerful and unique applications. The applications created on Appian's platform help companies drive digital transformation and competitive differentiation.

For more information, visit www.appian.com